APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/766,882	01/30/2004	Sandro Grech	059643.00316	4108

32294 7590 01/28/2008 SQUIRE, SANDERS & DEMPSEY L.L.P. 14TH FLOOR 8000 TOWERS CRESCENT TYSONS CORNER, VA 22182	**EXAMINER** SHEDRICK, CHARLES TERRELL

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
01/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/766,882	GRECH ET AL.
	Examiner	Art Unit	
	Charles Shedrick	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>29 October 2007</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-16</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-16</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 10/29/07 has been entered.

Response to Arguments

Applicant's arguments filed 10/29/07 have been fully considered but they are not persuasive.

With respect to the claim language the Examiner presents the following explanation in an effort

to clarify the claim interpretation and the rejection as follows.

2.   **performing an authentication procedure**

The claims recite "performing an authentication procedure", which refers to any part or role

involved in at least the authentication method and not necessarily the authentication result. A

procedure generally refers to the method rather than the result. The claim further indicates

"performing" an authentication procedure which implies being in the act of and not necessarily

the completion of. The Examiner respectfully notes that the Applicant assertion of "pre"

indicating something that precedes another thing is correct. However, the intention of the

Examiner is to communicate that the pre-authentication (i.e., MN-FA challenge extension

contained in the ProxyRtAdv which is used for authentication and authorization purposes) is

actually considered as the initial phase of "performing" the authentication procedure although it

occurs before the authentication "process" is completed.

3.   Packet Data Protocol Establishment

The Examiner respectfully notes that a Packet data protocol as discussed herein is interpreted as

frame relay, IP, x.25, etc. The claims recite simultaneously "performing a packet data protocol

session" (i.e., performing IP, frame relay, X.25, etc. protocol session). The claims do not

explicitly claim the PDP context establishment. The abstract (i.e., at least the abstract) recites the

ability to prevent the disruption of **ongoing** internet (e.g., IP) session. Therefore as a basis for

operating in an ongoing internet session (i.e., performing a packet data protocol session) and

accomplishing a handover to a second network in which an authentication procedure must take

place. A careful examination of claim 1 would clearly show that there is nothing the clearly

identifies when the data protocol session establishment procedure begins. Accordingly, based on

the fact that the internet sessions are "ongoing", one of ordinary skill in the art would recognize

the TCP sessions (i.e., packet data) would also be "ongoing (e.g., TCP three way handshake,

open connection/closed connection on various ports etc.). The performing of a packet data

protocol session establishment procedure is actually occurring simultaneously with the

authentication procedure since the claim language opens the invention to any IP (i.e., packet

data) session procedure and the authentication procedure would begin at some point during an

"ongoing" internet session. The Applicant asserts on page 15 of the remarks that " In Parikh

only the pre-authentication process is carried out while still being attached to the first

communication network , while in the recitations of claim 1, the pre authentication **and the PDP**

context establishment are carried out while still being attached to the first communication

network". It is important that the Applicant notes that nowhere in the claim language is "PDP

context establishment" recited. The claim language opens the interpretation to any PDP (e.g., IP,

FrameRelay) establishment. The Examiner respectfully notes that Applicants repeated assertions

of **PDP context** are not explicitly stated in the claims. There are no indications in the claim

language that establishes **when** the "performing a packet data protocol session establishment

procedure" begins. It appears that the Applicant is arguing that the **PDP context** establishment

initiates the PDP establishment, however the claim language does not make the distinction.

Again, although the claims are interpreted in light of the specification, limitations from the

specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26

USPQ2d 1057 (Fed. Cir. 1993).

Regarding claim 10, Parikh describes the Spurious Handoff triggers (e.g., which cause the noted

ping pong affect) in section 3.3. e.g., a terminal waiting a short time after the loss of a first

network before initiating handoff to a second network. The solution which as addresses claims

10 as noted specifically in the previous remarks in section 4.2.1.

Therefore, the rejection is maintained as proper

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this
> or a foreign country, before the invention thereof by the applicant for a patent.

2.   Claims **1-15** are rejected under 35 U.S.C. 102(a) as being anticipated by **Parikh et al.**

(see PTO-892 Non-patent Literature section U)

Consider **claim 1**, Parikh et al. teaches the method for ensuring continuity of a

communication session when a user equipment hands over from a first communication network

(i.e., WLAN) to a second communication network (i.e., CDMA2000) comprising: performing an

authentication procedure for a packet data session with the second communication network while

the user equipment is still connected to the first communication network (**abstract,**

introduction, section 4.1 and figure 4); and simultaneously performing a packet data protocol

session establishment procedure with the second communication network while the user

equipment still connected to the first communication network (**abstract , introduction, section**

4.1 and figure 4).

Consider **claim 2** and **as applied to claim 1 above**, Parikh et al. teach a method as

claimed in claim 1, wherein the performing of the authentication procedure comprises

authenticating the second communication network (i.e., the CDMA2000) by the user equipment

(i.e., authentication challenge)(**section 4.1 and figure 4**).

Consider **claim 3** and **as applied to claim 2 above**, Parikh et al. teach a method as

claimed in claim 2, wherein the step of performing the authentication procedure comprises

authenticating the user equipment by the second communication network (i.e., the authentication

challenge) (**section 4.1 and figure 4**).

Consider **claim 4** and **as applied to claim 1 above**, Parikh et al. teach a method as

claimed in claim 1, further comprising: providing the first communication network comprising a

Wireless Local Area Network (WLAN) and the second communication network comprising a

cellular network (i.e., CDMA2000)(**section 1**).

Consider **claim 5** and **as applied to claim 1 above**, Parikh et al. teach a method as

claimed in claim 1, wherein the performing of the authentication procedure comprises sending

information by a user equipment for authentication and packet data session establishment,

wherein the information travels either as a separate IP package or is piggybacked with existing signaling (**section 4.1 and figure 4**).

Consider **claim 6** and **as applied to claim 1 above**, Parikh et al. teach a method as claimed in claim 1, further comprising: configuring a gateway node (i.e., AR)(**figure 4.1**) between the first communication network and the second communication network to act as an access router for the first communication network and to host the packet data session in the second communication network (**section 4.1 and figure 4**).

Consider **claim 7** and **as applied to claim 1 above**, Parikh et al. teach a method as claimed in claim 1, further comprising: releasing a packet data session if a user equipment does not handover to the second communication network within a predetermined time thus requiring the user equipment to repeat the authentication procedure if the user equipment is moving towards the second communication network for a specified time (i.e., a gap in coverage) (**section 4.2.1**).

Consider **claim 8** and **as applied to claim 1 above**, Parikh et al. teach a method as claimed in claim 1, further comprising: (i) sending by a user equipment a handover trigger indication to a gateway node in the second communication network, wherein the handover trigger indication comprises user equipment identification parameters and a packet data protocol profile (**section 4.1 and figure 4**); (ii) sending by a gateway node the user equipment identification parameters and the packet data protocol profile to a serving node in the second cellular communication network (**section 4.1 and figure 4**); (iii) contacting by the serving node a home location register to obtain user equipment authentication parameters (**section 4.1 and figure 4**); (iv) sending by the serving node a packet data protocol profile request to the gateway

node (**section 4.1 and figure 4**); (v) responding by sending by the gateway node a packet data protocol profile response to the serving node(**section 4.1 and figure 4**); (vi) sending by the serving node authentication information to the gateway node(**section 4.1 and figure 4**); (vii) sending the gateway node the authentication information to the user equipment(**section 4.1 and figure 4**); (viii) authenticating by the user equipment the second communication network(**section 4.1 and figure 4**); (ix) sending by the user equipment a response to the serving node and moving the user equipment into the second cellular communication network(**section 4.1 and figure 4**);

Consider **claim 9** and **as applied to claim 1 above**, Parikh et al. clearly show and disclose a method as claimed in claim 1, further comprising: (i) sending by a user equipment a handover trigger indication to a gateway node in the second communication network(**section 4.1 and figure 4**); (ii) sending by the gateway node a protocol data unit notification request to a serving node in the second communication network(**section 4.1 and figure 4**); (iii) contacting by the serving node a home location register (i.e., HA) to obtain user equipment authentication parameters(**section 4.1 and figure 4**); (iv) sending by the serving node a proxy authentication and a ciphering request to the gateway node(**section 4.1 and figure 4**); (v) converting by the gateway node authentication information in the ciphering request which is then sent to the user equipment(**section 4.1 and figure 4**); (vi) responding by the user equipment with an authentication message which is sent to the gateway node(**section 4.1 and figure 4**); (vii) converting by the gateway node the authentication message from the user equipment and sending a proxy authentication and a ciphering response to the serving node(**section 4.1 and figure 4**); (viii) sending by the serving node a protocol data unit notification response to the gateway node(**section 4.1 and figure 4,conclusion**); (ix) sending by the serving node a create packet data

protocol request to the gateway node(**section 4.1 and figure 4, conclusion**) (i.e., see "network

initiated bearer setup"); (x) sending by the gateway node a create packet data protocol response

to the serving node(**section 4.1 and figure 4,conclusion**) (i.e., see "network initiated bearer

setup"); and (xi) replying by the gateway node to the handover trigger indication sent by the user

equipment by sending a handover trigger response to the user equipment(**section 4.1 and figure

4**).

Consider **claim 10**, Parikh et al. clearly show and disclose a method for ensuring

continuity of a communication session, the method comprising: handing over by a user

equipment from a first communication network (i.e., WLAN) (**figures 1 and 2**) to a second

cellular communication network (IMT-2000 Radio Network) (**figures 1 and 2**), and when the

user equipment hands over from the first communication network to the second communication

network (**section 4.1 and figure 4**), maintaining an attachment of the user equipment to the first

communication network after the user equipment moves away from a coverage area of the first

communication network for a predetermined time in order to allow the user equipment to return

to the first communication network without having to repeat an authentication procedure and a

packet data session establishment procedure before handing over to the second network (i.e., this

prevents the spurious handoff triggers) ((**sections 3.3- 4.2.1**).

Consider **claim 11** and **as applied to claim 10 above**, Parikh et al. teach a method as

claimed in claim 10, further comprising: releasing a packet data session if the user equipment

does not handover to the second cellular communication network within the predetermined time

thus requiring the user equipment to repeat the authentication procedure if the user equipment is

moving towards the second communication network for a specified time (i.e., a gap in coverage

and other areas for potential spurious handoff triggers) (**section 4.2.1**).

Consider **claim 12** and **as applied to claim 10 above**, Parikh et al. teach a method as

claimed in claim 1, further comprising: (i) sending by a user equipment a handover trigger

indication to a gateway node in the second communication network, wherein the handover

trigger indication comprises user equipment identification parameters and a packet data protocol

profile (**section 4.1 and figure 4**); (ii) sending by a gateway node the user equipment

identification parameters and the packet data protocol profile to a serving node in the second

cellular communication network (**section 4.1 and figure 4**); (iii) contacting by the serving node

a home location register to obtain user equipment authentication parameters (**section 4.1 and**

figure 4); (iv) sending by the serving node a packet data protocol profile request to the gateway

node (**section 4.1 and figure 4**); (v) responding by sending by the gateway node a packet data

protocol profile response to the serving node(**section 4.1 and figure 4**); (vi) sending by the

serving node authentication information to the gateway node(**section 4.1 and figure 4**); (vii)

sending the gateway node the authentication information to the user equipment(**section 4.1 and**

figure 4); (viii) authenticating by the user equipment the second cellular communication

network(**section 4.1 and figure 4**); and (ix) sending by the user equipment a response to the

serving node and moving the user equipment into the second communication network(**section**

4.1 and figure 4);

Consider **claim 13** and **as applied to claim 10 above**, Parikh et al. teach a method as

claimed in claim 1, further comprising: (i) sending by a user equipment a handover trigger

indication to a gateway node in the second communication network(**section 4.1 and figure 4**);

(ii) sending by the gateway node a protocol data unit notification request to a serving node in the

second cellular communication network(**section 4.1 and figure 4**); (iii) contacting by the serving

node a home location register to obtain user equipment authentication parameters(**section 4.1**

and figure 4); (iv) sending by the serving node a proxy authentication and a ciphering request to

the gateway node(**section 4.1 and figure 4**); (v) converting by the gateway node authentication

information in the ciphering request which is then sent to the user equipment(**section 4.1 and**

figure 4); (vi) responding by the user equipment with an authentication message which is sent to

the gateway node(**section 4.1 and figure 4**); (vii) converting by the gateway node the

authentication message from the user equipment and sending a proxy authentication and a

ciphering response to the serving node(**section 4.1 and figure 4**); (viii) sending by the serving

node a protocol data unit notification response to the gateway node(**section 4.1 and figure**

4,conclusion); (ix) sending by the serving node a create packet data protocol request to the

gateway node(**section 4.1 and figure 4**) (i.e., see "network initiated bearer setup"); (x) sending

by the gateway node a create packet data protocol response to the serving node(**section 4.1 and**

figure 4, conclusion) (i.e., see "network initiated bearer setup"); and (xi) replying by the

gateway node to the handover trigger indication sent by the user equipment by sending a

handover trigger response to the user equipment(**section 4.1 and figure 4**).

Consider **claim 14**, Parikh et al. clearly show and disclose a communication system

(**abstract and introduction**) comprising: a user equipment; a first communication network and a

second cellular communication network, the system being configured to enable continuity of a

communication session when a user equipment moves from a coverage area of the first

communication network to a coverage area of a second cellular communication network

(**abstract, introduction, section 4.1 and figure 4**), and to simultaneously perform an

authentication procedure for a packet data session with the second cellular communication

network and a packet data protocol session establishment procedure with the second cellular

communication network, while the user equipment is still attached to the first communication

network(**abstract , introduction, section 4.1 and figure 4**.

Consider **claim 15**, Parikh et al. teach the communication system (**figures 1-4**) for

ensuring continuity of a communication session when a user equipment hands over from a first

communication network to a second cellular communication network (**abstract and

introduction**), the communication system comprising: first performing means for performing an

authentication procedure for a packet data session with a second communication network while

still being attached to a first communication network (**abstract , introduction, section 4.1 and

figure 4**); and second performing means for simultaneously perform a packet data protocol

session establishment procedure with the second cellular communication network while still

being attached to the first communication network(**abstract , introduction, section 4.1 and

figure 4**).

Consider **claim 16**, Parikh et al. teach the communication system (**figures 1-4**),

comprising an authentication unit configured to conduct an authentication procedure for a packet

data session between a first and second communication networks when a user equipment hands

off from the first communication network to the second communication network (**abstract ,

introduction, section 4.1 and figure 4**), the authentication procedure being conducted while the

user equipment is still attached to a first communication network(**abstract , introduction,

section 4.1 and figure 4**); and an establishment unit configured to simultaneously performing a

packet data session establishment procedure with the second communication network while still

being attached to the first communication network(**abstract , introduction, section 4.1 and**
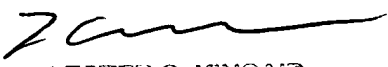
figure 4).

Conclusion

3.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

Gao et al. US Patent Pub. No: 2004/0067754 A1 teaches the claimed in invention see at least

paragraphs 0033-0047)

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Charles Shedrick whose telephone number is (571)-272-8621.

The examiner can normally be reached on Monday thru Friday 8:00AM-4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kincaid Lester can be reached on (571)-272-7922. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Charles Shedrick
AU 2617
January 16, 2008